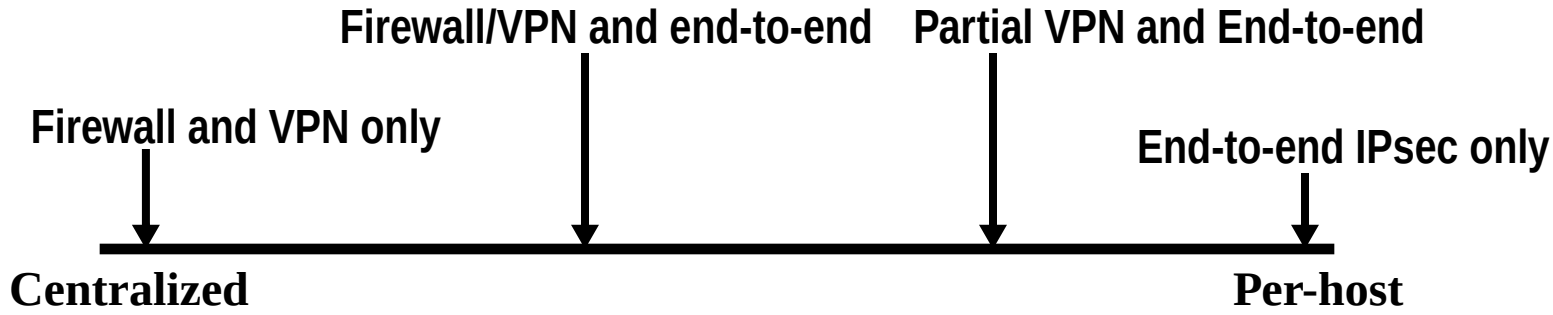
What Will Probably Happen

- **Both end-to-end IPsec and firewalls/ VPNs will co-exist.**
- **Consider an example spectrum:**



- **A particular solution will lie somewhere along the spectrum.**

Sun microsystems

Central Administration

- **Single Point of {*Control*, Failure}.**
- **In a large organization, workstations/ PCs/etc. go through a "filling station."**
- ***People would like to eliminate that eventually and plug in out of the box.***

Sun microsystems

VPN Construction

- **End-to-end encryption protects just as well as router-to-router encryption.**
- **Some VPN implementations protect different traffic flows.**
- **Why not save router cycles and let the hosts and users determine that themselves?**
- ***Do you trust users to do that themselves?***

Sun microsystems

Preventing Outbound Access

- **Is this really a feature?**
- ***Yes it is! I might not trust my users.***
- **If so, you could mandate nothing but AH, and apply normal monitoring tools.**
- ***But I thought you said you could apply per-socket policy above-and-beyond systemwide policy?***

Sun microsystems

Preventing Attacks

- Apply per-endpoint policy properly.
- For example, an NFS fileserver might have:
  - NFS traffic uses AH and per-host certificates. (Use NFS/GSS for encryption.)
  - All other traffic is encrypted with user@fqdn certificates.
- *But how do you distribute this policy?*

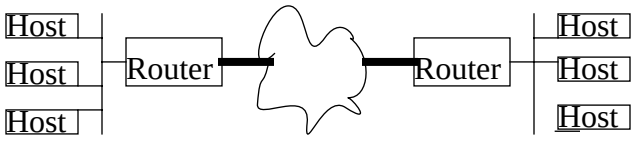
Sun microsystems

End-to-End IPsec Policy

- **Systemwide Policy**
  - **Rules that are applied to a host's traffic.**
  - **Example: "All traffic with foreign port 23 must be encrypted, with source SA certificate identity of *user*@this-host's-domain."**
- **Per-Endpoint (e.g. socket) Policy**
  - **Can override (for privileged users) or enhance systemwide policy.**

End-to-End IPsec

- **Instead of building router-to-router tunnels, protect your traffic end-to-end.**



VIRTUAL PRIVATE NETWORK (VPN)

END-TO-END PROTECTION

- **Once the packet leaves the host, it is protected, and you don't have to trust your network.**

Sun microsystems

Problems That Firewalls Solve

- **Protecting a set of machines from attack.**
- **Restricting outbound access to the Net, except via a proxy.**
- **In more advanced firewalls, VPN construction.**
- **Central administration of policy and access control.**

Sun microsystems

My Biases

- **I lean toward end-to-end IPsec solutions.**
  - **In other words, I'd *like* to answer my question with "No."**
- **I will try and present both "*Yes*" and "No" answers fairly.**
- **I want to encourage discussion, debate, and questions.**

Sun microsystems

Will We Need Firewalls in the Future?

Daniel L. McDonald

Software Engineer - Solaris Internet Engineering
Sun Microsystems, Inc.

Sun microsystems